ABSTRACT OF THE DISCLOSURE

Mapping is carried out at a point on an elliptic curve to be utilized for elliptic encryption based on identity information (ID information) of each entity and a mapping value is set to be a public key of the entity. By using the mapping value and secret information, a secret key of each entity is generated. The entity generates a common key to be used for an encrypting process and a decrypting process by utilizing the self-secret key and the public key to be the mapping value obtained by mapping at a point on the elliptic curve based on ID information of a communication participate. In this case, pairing on the elliptic curve is utilized.